REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-34 are pending in the application. The Examiner additionally stated that claims 1-34 are rejected. By this communication, claims 6, 13, 27, and 31 are cancelled and claims 1, 7-8, 22-23, and 29-29 are amended. Hence, claims 1-5, 7-12, 14-26, 28-30, and 32-24 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-5, 10-11, 13-22, 25-28, and 31-34 under 35 U.S.C. 103(a) as being unpatentable over Yup et al., US PGP No. 20020191784 (hereinafter, "Yup"), in view of Laurenti, US Patent No. 6795930 (hereinafter, "Laurenti"). Applicant respectfully traverses the Examiner's rejections.

As per claims 1, 22, and 28, the Examiner wrote that Yup teaches an apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said one of the cryptographic operations comprises: [see paragraphs 0038-0039]

- a plurality of CFB block cryptographic operations performed on a corresponding plurality of input text blocks; [see paragraph 0040]
- [CFB] mode logic, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to update pointer registers and

intermediate results for each of said plurality of [CFB] block cryptographic operations; and [see paragraph 0025]

- execution logic, operatively coupled to said [CFB) block pointer logic, configured to execute said one of the cryptographic operations. [see paragraph 0041]

The Examiner conceded that Yup is not explicit in teaching CFB block cryptographic operations, but that Yup teaches cryptographic operations on multiple successive blocks of text. The Examiner noted that Yup does not expressly state that these cryptographic operations are of cipher block chaining mode, but that as is evident in Applicant's disclosure on paragraph 0012 of the specification, it is well known that all symmetric key algorithms employ the same types of modes, and that ECB, CBC, CFB, and OFB are examples that Applicant discloses. Based on this, the Examiner deemed it obvious for one of ordinary skill in the art to implement CFB or any other block cipher mode in conjunction with the system/apparatus taught by Yup.

The Examiner also noted that Yup is not explicit in teaching that the computing device is a pipeline microprocessor and, for this limitation, the Examiner relies the Laurenti reference, directing Applicant's attention to FIGURE 6 in which Laurenti teaches a pipeline microprocessor.

The Examiner thus concluded that it would have been obvious at the time of the invention to one of ordinary skill in the art to combine the teaching of Yup above to include the pipeline processor taught by Laurenti in order to reduce power consumption of the computing device by allowing it to operate in a lower power mode during times of inactivity (see Laurenti, col. 1, lines 34-39).

In response to Applicant's arguments submitted in the previous communication, the Examiner noted that the arguments were considered, but are moot in view of the new grounds of rejection.

Applicant respectfully disagrees with the Examiner's characterization and understanding of the teachings of Yup, Laurenti, and of the invention as recited in particular in claims 1, 22, and 28. Thus, the following points are submitted in traversal of the rejections.

First, one skilled in the art will concur that a microprocessor includes an understood set of functions and logic elements. Generally speaking, a microprocessor is understood by those in the art to microprocessor be a programmable digital electronic component that incorporates the functions of a central processing unit (CPU) on a single integrated circuit (IC). The aforementioned aspects of the microprocessor according to the present invention are very adequately disclosed within the instant application to include the ability to fetch and execute instructions that have been provided in an application program, to perform address translation, to load and store variables from/to memory, etc. As such, a microprocessor differs from a coprocessor, which is conventionally understood to supplement the functions of the CPU. Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption, as has been discussed in the instant application. Coprocessors require the host main processor to fetch the coprocessor instructions and handle all other operations aside from the coprocessor functions. Accordingly, and as Applicant has discussed in the instant application and in the previous response, a microprocessor is not a coprocessor, nor is a coprocessor a microprocessor. Applicant has discussed the existence and disadvantages of present day cryptographic coprocessors, and has provided the present invention to overcome the disadvantages of such.

The apparatus of Yup is not even a coprocessor. It is a circuit. And as such, Yup's circuit falls into that class of devices that are employed to offload operations from a host processor, examples of which Applicant discussed in the instant disclosure. Certainly, Yup does not disclose, suggest, allude to, or even hint that his circuit be construed or combined with other circuits to yield a coprocessor, much less a microprocessor.

Applicant does not dispute that the microprocessor taught by Laurenti is a pipeline microprocessor. And as indicated by the Examiner and as is discussed with reference to FIGURE 6, Laurenti's pipeline microprocessor includes pipeline stages that are similar to those of the present invention. Both Laurenti's microprocessor and the microprocessor according to the present invention are pipeline microprocessors.

Applicant wishes to respectfully note, however, that the question is not whether one can configure a microprocessor as a series of pipeline stages, but whether a general purpose pipeline microprocessor, such as is exemplified by Laurenti, can be programmed by a single instruction within an application program executing thereon, to perform an extremely complex cryptographic operation, such as encrypting or decrypting a multi-block message according to the Advanced Encryption Standard. As one skilled in the art will appreciate, this type of operation, when performed on a general purpose microprocessor via calls to a dynamic link library (i.e., performing the cryptographic operation via software subroutines), literally thousands of sub-operations are required, and to atomically perform the cryptographic operation on a microprocessor, provisions must be provided for interrupts, exceptions, and the like, because it is entirely probable that execution of the cryptographic operation will be interrupted numerous times.

Applicant respectfully submits that the above reason is one of the many obstacles that has heretofore precluded the provision of an invention such as is recited in particular in claims 1, 22, and 28.

To further clarify that which is regarded as the present invention, Applicant has amended claims 1, 22, and 28 to recite a that the cryptographic instruction is prescribed according to the x86 instruction format, thus restricting the pipeline microprocessor to be according to the x86 architecture. Furthermore, to clarify that the cryptographic operation is performed on a microprocessor responsive to receipt of a cryptographic instruction, it is necessary that interrupting events be dealt with during execution. Accordingly, claims 1, 22, and 28 are amended to recite a bit, coupled to said execution unit, configured to indicate whether said one of the cryptographic operations has been interrupted by an interrupting event.

As Applicant's representative discussed with the Examiner via telephone on 10/06/2008, the above noted limitations distinguish the present invention over the cited references. Applicant further noted that numerous applications are pending or have been issued patents related to the product in which the present invention is embodied. The Examiner is assigned to three of these applications (serial nos. 10826814, 10826428, and

10826745) and Ms. Traore of the same GAU is assigned serial no. 10800983 and related application serial no. 10963427. Related applications 10800768 and 10674057 have issued. Application serial no. 10727973 has been allowed. And the remaining applications listed in the "Cross-Reference to Related Applications" section of the specification are at varied stages of prosecution.

It is respectfully submitted that Laurenti does not contemplate, suggest, or even hint that his pipeline microprocessor may be modified or configured to perform any sort of complex operation that requires numerous sub-operations to perform. Applicant respectfully submits that one skilled would treat the combination of Yup and Laurenti to yield a separate circuit or coprocessor to perform AES operations because neither of these two named references contemplate the performance of a complex cryptographic operation in the presence of interrupting events.

Accordingly, it is respectfully requested that the rejections of claims 1, 22, and 28 be withdrawn.

By this communication, claim 13 is cancelled, thereby rendering the rejection moot.

With respect to claims 2-5, 10-11, and 14-21, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup, Laurenti, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-5, 10-11, and 14-21.

With respect to claims 25-67, these claims depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Yup, Laurenti, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 25-26.

By this communication, claim 27 is cancelled, thereby rendering the rejection moot.

With respect to claims 32-34, these claims depend from claim 28 and add further limitations that are neither anticipated nor made obvious by Yup, Laurenti, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 32-34.

By this communication, claim 31 is cancelled, thereby rendering the rejection moot.

The Examiner also rejected claims 6-9, 12, 23-24, and 29-30, are rejected under 35 U.S.C. 103(a) as being unpatentable over Yup and Laurenti as applied to claim 1 above, and further in view of Sorimachi et al., US Patent No. 7184549.

Applicant respectfully traverses the rejections and notes that claims 7-9, 12, 23-24, and 29-30 depend from claims 1, 22, and 28 as appropriate, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, it is requested that the rejections of claims 7-9, 12, 23-24, and 29-30 be withdrawn.

By this communication, claim 6 is cancelled, thereby rendering the rejection moot.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-5, 7-12, 14-26, 28-30, and 32-24 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

10/22/2008

Date: _____